UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,160	02/26/2004	Hirotaka Yoshida	62807-167	9154

7590 03/20/2008

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
BAYOU, YONAS A	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
03/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/786,160	YOSHIDA ET AL.	
	Examiner	Art Unit	
	YONAS BAYOU	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4,5,10,12 and 24-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4,5,10,12 and 24-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 January 2008 and 26 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 01/28/2008.

2. Claims 1, 4-5, 10, 12 and 24-29 are pending.

3. Claims 2, 3, 6-9, 11 and 13-23 are cancelled.

4. Claims 1, 4, 5, 10 and 12 are amended.

5. Claims 24-29 are new.

6. Applicant's arguments have been fully considered but they are not persuasive.

7. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant, on page 10, line 7 – page 11, line 10, of the remarks, argues "in the method of claims 1, 10, 25 and 28, Gligor does not teach generating random-number blocks Ri (1=<i=<N+1) from a secret key, wherein the number of the random-number blocks Ri is greater than that of the plaintext blocks Pi,".

Examiner respectfully disagrees and asserts that Gligor discloses that the application of the selected parallel encryption mode 61 results in a plurality of hidden

ciphertext blocks 87 of .lambda.-bit length; the number of hidden ciphertext blocks 87 is greater by one than the number of the input plaintext blocks 21; i.e., it is n+1. For the example of FIG. 1, wherein n=4, the plurality of hidden ciphertext blocks 87 comprises n+1=5 blocks z.sub.1, z.sub.2, z.sub.3, z.sub.4, z.sub.5. These hidden ciphertext blocks 87 are submitted to a hidden ciphertext randomization step comprising, in one embodiment, applying a combination operation for the hidden ciphertext 84 to each hidden ciphertext block z.sub.I 87 and each .lambda.-bit element E.sub.I 83 of a sequence of n+1 elements for the hidden ciphertext. **[see, paragraph 159 and fig. 1].**

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1- 23 are rejected under 35 U.S.C. 102(b) as being anticipated by Gligor et al., Pub. No. US 2002/0048364 A1 (hereinafter Gligor).

Referring to claims 1, 10, 25 and 28, Gligor teaches an encryption apparatus for a common-key cipher, comprising:

a unit for generating a plurality of plaintext blocks Pi (1<=i<=N) resulting from separating a plaintext on a specific-length basis, the plaintext including a message M; **[paragraph 67];**

an encryption operation unit for generating a random-number blocks Ri (1<=i<=N+1) from a secret key, wherein the number of the random-number blocks Ri is greater than that of the plaintext blocks Pi **[paragraphs 47-48 and paragraphs 159; 160, lines 16-35;** E1=r0], and

performing an encryption operation for ciphertext blocks Ci (1<=i<=N) by using the plaintext blocks Pi (1<=i<=N) and the random-number blocks Ri (1<=i<=N), wherein number N of the random number blocks is the same as that of the ciphertext blocks; **[paragraphs 13, 18, 98, 125, 156, 163, 207, 210 and figs. 10-11;** hidden corresponding to encrypted]; and

a unit for generating a message-authentication-code of the ciphertext blocks Ci (1<=i<=N) by using the ciphertext blocks Ci (1<=i<=N) and the random-number blocks Ri (where 2=<i=<N+1) among the generated random-number blocks Ri, wherein the number N of the random-number blocks is the same as that of the ciphertext blocks **[paragraphs 13, 18, 98, 125, 156, 163, 207, 210 and figs. 10-11]**; and

an output unit for generating and outputting a ciphertext C comprising the ciphertext blocks and the message-authentication-code **[paragraph 12, lines 1-8, 16-**

23 and paragraphs 13-15; integrity check/MDC function corresponding to MAC/ authentication operation].

Referring to claims 4 and 26, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit is configured to perform the encryption operation by using an exclusive-OR logical sum, and to output the ciphertext blocks having a length the same as that of the plaintext blocks; and **[paragraphs 13, 18 and 157, lines 7-10]**; and

the message-authentication-code generation unit is configured to perform the authentication operation by using an arithmetic multiplication and an arithmetic addition **[paragraphs 13-14, 45, 60 and 160]**, and to output the message-authentication-code comprising message-authentication-code blocks C.sub.N+1 and C.sub.N+2 having a length two times longer than that of the ciphertext blocks **[paragraph 13, 18 and 21]**.

Referring to claims 5 and 27, Gligor teaches a program-storing medium and an encryption apparatus for a common-key cipher, wherein

the encryption operation unit is configured to perform the encryption operation by using an exclusive-OR logical sum, and to output the ciphertext blocks having a length the same as that of the plaintext blocks; and **[paragraphs 13, 18 and 157, lines 7-10]**; and

the message-authentication-code generation unit is configured to perform an authentication operation by a multiplication on a finite field **[paragraphs 13-14, 45, 60 and 160]**, and to output the message-authentication-code comprising message-authentication-code blocks C.sub.N+1 and C.sub.N+2 having a length two times longer than that of the ciphertext blocks **[paragraph 13, 18 and 21]**.

Referring to claims 12 and 29, Gligor teaches the decryption apparatus for a common-key cipher , wherein the decrvption operation unit does not perform the decrvption operation, if the authentication operation has failed **[paragraph 209;** rejecting corresponding to does not perform the decrvption operation].

Referring to claim 24, Gligor teaches the decryption apparatus for a common-key cipher, wherein:

the message-authentication included in the ciphertext has a length two times longer than the ciphertext blocks **[paragraph 13, 18 and 21]**;

the authentication operation unit is configured to perform the authentication operation by using an arithmetic multiplication **[paragraphs 13-14, 45, 60 and 160]**, and outputs the message-authentication-code comprising message-authentication-code blocks Cn+I and Cn+2, wherein the message-authentication-code has a length two times longer than that of the ciphertext blocks **[paragraph 13, 18 and 21]**; and

the decryption operation unit is configured to perform the decryption operation by using an exclusive-OR logical sum, and to output the plaintext blocks having a length the same as that of the ciphertext blocks **[paragraphs 13, 18 and 157, lines 7-10]**.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2134

03/12/2008

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134